PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PF020092	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP 03/50319	International filing date *(day/month/year)* 18.07.2003	Priority date *(day/month/year)* 24.07.2002
International Patent Classification (IPC) or both national classification and IPC H04N7/16		
Applicant THOMSON LICENSING S.A. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 2 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
09.02.2004	19.10.2004
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Cakiroglu, S Telephone No. +49 89 2399-7612

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP 03/50319

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1, 3-7	as originally filed
2, 2a	received on 23.06.2004 with letter of 14.06.2004

Claims, Numbers

1-12	as originally filed

Drawings, Sheets

1/1	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-12
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-12
Industrial applicability (IA)	Yes:	Claims	1-12
	No:	Claims	

2. Citations and explanations

   see separate sheet

1. Reference is made to the following documents:
   D1: US-A-4 890 322 (RUSSELL JR THOMAS L) 26 December 1989 (1989-12-26)
   D2: US 2001/0036271 A1 (JAVED SHOEB M) 1 november 2001 (2001-11-01)
   D3: WO 00 11867 A (MORENO ROLAND ; INNOVATRON SOCIETE ANONYME (FR)) 2 march 2000 (2000-03-02)

2. The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1-12 does not involve an inventive step in the sense of Article 33(3) PCT.

   Document D1, which is considered to represent the most relevant state of the art, discloses a method of distributing encrypted audiovisiual programs to user terminals (claim 6; abs.), in which different programs are encrypted with the aid of different keys (col. 5 lines 59-61). The method described therein comprises a step of initiating a telephone communication between the user terminal and a central service point, and during this connection transmitting the keys to the user terminal (claim 1; fig.1; col. 2 lines 24-28; col. 5 lines 31-35), in a manner synchronized with the distribution of the encrypted programs (col. 2 lines 20-25; col. 5 lines 20-35). It should be noted that the wording of the claim allows broad interpretation of the term "synchronization", which includes the synchronization as disclosed by D1 (where users need to initiate a phone call within the time period specified by the displayed information).

   The subject-matter of independent claim 1 differs from the method disclosed in D1 in that successive portions of the programme are encrypted using different keys. The objective technical problem to be solved by the distinguishing feature of the invention may therefore be regarded as how to provide a method for encrypting an audiovisual programme with multiple keys.

   However, this feature has already been employed for the same purpose in document D2, which discloses in the same technical field a method of dividing data comprising at least a video and an audio file into plurality of segments, encrypting each segment with a different key, and sending the user terminal the decryption keys (claims 17, 18; abs.; par. 0017, 0018, 0090). Furthermore, D2 also mentions that the reception of decryption keys is synchronized with the display of the audiovisual programme (par. 0098). It would be obvious to the person skilled in the art, namely when the same result is to be achieved, to apply this feature with corresponding effect to a method according to document D1, thereby

arriving at a method according to claim 1.

For the sake of completeness, it is mentioned that D3 also discloses, in the same technical field, a method distributing encrypted audio-video signal, where the decryption keys (included in a certificate) are sent to the users via a phone connection (claims 1, 2; abs.; page 2 line 28 - page 3 line 21; page 6 line 33 - page 7 line 1; page 8 lines 23-25). Since the missing features (encrypting different portions of the programme with different keys, and synchronizing the distribution of keys wit the distribution of the encrypted content) are already known from the disclosure of D2, the person skilled in the art would also be able to combine D2 and D3 to arrive at a method according to claim 1.

The subject-matter of claim 1 does therefore not involve an inventive step (Article 33(3) PCT).

3. The subject-matter of: independent claim 6 corresponds in terms of decoder (that receives and decodes data that has been distributed according to claim 1) features; independent claim 11 corresponds in terms of decoding method features; and independent claim 12 corresponds in terms of decryption routine to that independent claim 1. The supplementary feature of claim 12, that the call center has a predetermined call number, can only be regarded as a mere design matter. Therefore, the objections raised in respect of claim 1, also apply, mutatis mutandis, to independent claims 6, 11, and 12. Thus, they do not meet the requirements of Article 33 PCT.

4. The additional feature of dependent claims 2 and 10 (telephone communication utilizes an Internet protocol) is known from the disclosure of D3 (page 5 lines 29-35; page 6 lines 16-18). Thus claims 2 and 10 do not meet the requirements of Article 33 PCT.

5. The rest of the dependent claims relate to well-known design matters (synchronisation codes being transmitted to the user terminal; billing done according to the duration of the telephone communication; call center receiving telephone calls of an operator), and do not seem to contain any technical features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of inventive step.

transmitted by the central computer only after recognition of a serial number specific to the relevant box. The periodicity of transmission of the new code is for example monthly and the connection lasts for only a few seconds, so that the telephone line need only be tied up for a very short duration and frequency.

This technique is suitable for an overall subscription for a given period and requires complicated management of the subscriptions. It does not allow billing adapted in a simple manner to the programmes actually viewed by a user.

Patent US-4,890,322 describes a service for distributing announcement messages which is used to control TV signals, programme by programme. The enciphered signals sent are deciphered at the level of each subscriber by a deciphering unit, by virtue of the use of a nondedicated telephone service line. With each order from a subscriber, the deciphering unit automatically transmits the subscriber's request to the distribution service via the telephone service line, and receives in return, via this same line, coded key information necessary for deciphering the desired programme. The key information obtained is used for the duration of the programme ordered. By way of example, the description mentions a deciphering key transmitted to the subscriber in the form of a message repeated for three seconds, this key being in the form of a number consisting of coded numerical values which may be used to fix the coefficients of a signal filter.

This method makes billing per programme possible without, however, allowing finer billing (for example to view a given part of a broadcast), while requiring complicated management of billing.

(p. 2a)

To improve the fineness of control on the part of users, provision may be made for the independent transmission of parts of programmes, each being able to form the subject of a specific request. Thus, depending on the availability thereof, a user may decide to view a first part of a film on a first evening, then a second part on another evening. However, such a solution yet further complicates the management of transmission and billing, all the more so the more elaborate the offerings - for example if they allow a viewer to choose the duration of each of the parts.

Document US2001/0036271 relates to a technique for securely distributing digital content for short-term use. A subscriber device is able to receive selected digital data files, including video and audio files, by downloading them from digital content servers. In the latter, the selected files are divided into successive segments, which are encrypted with a plurality of encryption keys. The resulting encrypted segments are transmitted to the subscriber device and are stored locally therein. Also, a copy of the decryption keys is transmitted to the subscriber device as and when the subscriber is authorised thereto, but those received keys are not stored in local storage and are exploited instead in a short delay.

Though that technique may provide improved security with full control from servers administered by the content owners, while avoiding complete retransmission of the requested program each time a video is played, it remains limited in the billing flexibility.

Prior art WO-00/11867 discloses a method enabling to deliver in a certified way a sequence of data, which may include audio, video or textual data. Therein, an apparatus provided with a decryption smart card (and possibly an invoicing smart card) is connected to a remote server. That server sends to the apparatus, on request, a stream of compressed and encrypted digital signals corresponding to the chosen sequence. That sequence is associated with invoicing information that the apparatus transmits to a remote payment site. The payment site provides in return a cryptographic certificate, on which a cryptographic key for deciphering the data may depend or not. The apparatus, via the smart card, checks the conformity of the certificate and, in case of acknowledgement, delivers the decompressed and decrypted data to the user.

Such an achievement, though secured and reliable billing process, requests preliminary local storing of the encrypted data to be exploited as well as of the decryption key. It may thus take significant storing space and limit the possibilities for the data to be played. Also, it does not offer finer billing potential than the other known techniques mentioned above.